BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 600 188**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **86 08655**

(51) Int Cl⁴ : G 06 K 19/06.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 16 juin 1986.

(30) **Priorité :**

(43) **Date de la mise à disposition du public de la demande :** BOPI « Brevets » n° 51 du 18 décembre 1987.

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *BULL CP8.* — FR.

(72) **Inventeur(s) :** Michel Hazard et Michel Ugon.

(73) **Titulaire(s) :**

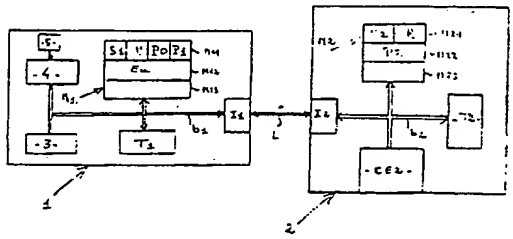
(74) **Mandataire(s) :** Colombe, Bull S.A.

(54) Procédé d'habilitation d'un milieu extérieur par un objet portatif relié à ce milieu.

(57) L'invention a pour objet un procédé d'habilitation d'un milieu extérieur par un objet portatif relié à ce milieu.

L'objet portatif 1 et le milieu extérieur calculent respectivement des premier R1 et second R2 résultats qui prennent en compte au moins une donnée variable Eu prélevée dans l'objet portatif 1 et modifiée après chaque utilisation de l'objet portatif 1. Ces deux résultats sont comparés dans l'objet portatif 1.

L'invention s'applique à l'habilitation d'un terminal par une carte de crédit.



FR 2 600 188 - A1

Vente des fascicules à l'IMPRIMERIE NATIONALE, 27, rue de la Convention — 75732 PARIS CEDEX 15

Procédé d'habilitation d'un milieu extérieur par un objet portatif relié à ce milieu.

L'invention a pour objet un procédé d'habilitation d'un milieu extérieur par un objet portatif relié à ce milieu.

L'invention permet notamment de faire habiliter un milieu extérieur tel qu'un système de délivrance d'un service ou d'autorisation d'accès par un objet portatif tel qu'une carte à mémoire comprenant des circuits de traitement.

Il est connu de systèmes d'habilitation où le milieu extérieur s'assure que l'objet portatif qui sollicite l'accès à ce milieu est bien habilité pour obtenir un tel accès.

Le principe de ces systèmes d'habilitation consiste à entrer depuis l'extérieur un nombre aléatoire dans l'objet portatif, à faire calculer un résultat au moins fonction de ce nombre aléatoire par les circuits de traitement de l'objet portatif, à extraire ce résultat de l'objet portatif et à le comparer avec un résultat calculé par le milieu extérieur et qui est au moins fonction de ce même nombre aléatoire. S'il y a concordance entre ces deux résultats, le milieu extérieur valide l'accès demandé par l'objet portatif.

La prise en compte d'un nombre aléatoire permet de calculer un résultat différent à chaque utilisation de l'objet portatif afin d'éviter qu'un fraudeur ne puisse simuler un faux objet portatif à partir de la connaissance d'un résultat antérieur ou ne puisse précalculer à l'avance un tel résultat.

Un tel système d'habilitation est notamment décrit dans le brevet français N° 2 469 760 de la demanderesse.

Il est important de noter que dans un tel système d'habilitation, c'est le milieu extérieur qui a la

maîtrise du dialogue pour déterminer si l'objet portatif est habilité ou non à dialoguer avec le milieu extérieur.

Cependant, il apparait nécessaire pour des raisons de confidentialité ou de sécurité, que l'objet portatif puisse aussi être assuré que le milieu extérieur est bien habilité pour dialoguer avec lui, notamment lorsque la liaison entre l'objet et le milieu est une liaison à distance.

Le but de l'invention est donc de donner la maîtrise de l'habilitation à l'objet portatif et non pas seulement au milieu extérieur. On pourrait penser qu'il suffit pour résoudre ce problème de prendre un système d'habilitation tel que décrit précédemment et de faire effectuer la comparaison des résultats par l'objet portatif et non plus par le milieu extérieur. Une telle solution n'a pas de sens, car il serait aisé de simuler un faux milieu extérieur en utilisant un résultat connu à l'avance étant donné que c'est le milieu extérieur qui est maître du nombre aléatoire transmis à la carte.

Il faut donc pour qu'un objet portatif puisse habiliter un milieu extérieur que le nombre aléatoire soit géré par l'objet portatif.

A cet effet, l'invention propose un procédé d'habilitation d'un milieu extérieur par un objet portatif relié audit milieu, du type consistant à faire respectivement calculer des premier et second résultats par des circuits de traitement de l'objet portatif et du milieu extérieur, ces calculs prenant au moins en compte une même donnée variable, caractérisé en ce qu'il consiste à prélever ladite donnée variable dans l'objet portatif et à faire vérifier la cohérence des deux résultats par l'objet portatif.

Selon un avantage important de l'invention, le milieu extérieur peut habiliter l'objet portatif selon un système d'habilitation de l'art antérieur, et l'objet portatif peut habiliter le milieu extérieur selon le procédé de l'invention. Autrement dit, il peut y avoir une habilitation mutuelle entre l'objet portatif et le milieu extérieur.

Selon un autre avantage de l'invention, l'objet portatif est constitué par une carte à mémoire normalisée.

D'autres avantages, caractéristiques et détails ressortiront de la description explicative qui va suivre faite en référence à la figure annexée donnée à titre d'exemple et qui représente de façon schématique les éléments essentiels d'un système d'habilitation permettant la mise en oeuvre du procédé conforme à l'invention.

Le système d'habilitation tel que représenté sur la figure est essentiellement constitué par un objet portatif tel qu'une carte à mémoire (1) et par un milieu extérieur (2) reliés l'un à l'autre en local ou à distance par une liaison (L) du type optique ou électrique.

La carte (1) comprend au moins une mémoire (M1), généralement du type programmable, des circuits de traitement (T1) tels qu'un microprocesseur et une interface d'entrée-sortie (I1). Ces différents circuits sont reliés entre eux par un bus (b1) de commande, d'adresse et de donnée. Une telle carte est notamment décrite dans les brevets français n° 2 401 459 et 2 461 301 de la demanderesse.

Le milieu extérieur est schématisé par un ensemble (2) qui comprend au moins une mémoire (M2), des circuits de traitement (T2), un dispositif d'entrée-sortie tel qu'un

clavier (CE2), et une interface d'entrée-sortie (I2). Ces différents circuits sont reliés entre eux par un bus (b2) de commande, d'adresse et de donnée. Bien entendu, en fonction de sa nature, cet ensemble (2) est équipé d'autres éléments ou circuits non représentés par souci de simplification.

La carte (1) est accouplable temporairement, en local ou à distance, au milieu extérieur (2) par les interfaces (I1, I2) et par la liaison (L) telle que décrite par exemple dans le brevet français n° 2 483 713 de la demanderesse.

La mémoire (M1) de la carte (1) se subdivise en trois zones de mémoire (M11, M12, M13).

La zone (M11) est inaccessible de l'extérieur de la carte (1). Elle contient des données confidentielles ou secrètes qui ne peuvent être traitées qu'en interne par les circuits de traitement (T1).

La zone (M12) dénommée zone de contrôle est accessible en lecture et en écriture par les circuits de traitement (T1) mais n'est accessible qu'en lecture depuis l'extérieur de la carte (1). Elle contient des informations dont le contenu évolue en fonction de l'utilisation de la carte (1).

Enfin la zone (M13) dénommée zone de travail est accessible en lecture et en écriture depuis l'extérieur de la carte (1) et par les circuits de traitement (T1).

La mémoire (M2) du milieu extérieur (2) se subdivise également en trois zones de mémoire (M21, M22, M23) ayant respectivement les mêmes conditions d'accès que les trois zones de mémoire de la mémoire (M1).

A titre d'exemple, la zone de mémoire (M11) de la carte (1) renferme au moins un code confidentiel (CC) attribué au titulaire de la carte (1) par un organisme habilité (non représenté), et une clé secrète (S1) inconnue du titulaire de la carte et spécifique du ou des services qui peuvent être délivrés au moyen de cette carte. Parallèlement, la zone de mémoire (M21) du milieu extérieur (2) renferme au moins une clé secrète (S2) spécifique de ce milieu. D'une façon générale, une habilitation entre une carte et un milieu extérieur ne peut être validée qu'à la condition que les clés secrètes (S1, S2) soient identiques ou satisfassent une relation prédéterminée.

Les zones de mémoire renferment des programmes nécessaires au fonctionnement de la carte et du milieu extérieur. Ces programmes seront précisés par la suite.

Supposons que la carte (1) est accouplée en local ou à distance au milieu extérieur (2), et que ce milieu extérieur (2) est un système ou un appareil susceptible de délivrer un service ou autoriser l'accès à un autre système.

La délivrance du service où l'autorisation d'accès est généralement donnée à la suite d'un dialogue préliminaire entre la carte et le milieu extérieur.

Ce dialogue préliminaire est constitué d'une ou plusieurs séquences d'échange d'informations entre la carte et le milieu pour effectuer des contrôles qui sont fonction de l'application envisagée et du degré de sécurité ou de confidentialité requis par cette application.

A titre d'exemple, un premier contrôle peut consister à s'assurer que l'utilisateur de la carte (1) en est bien le

titulaire. Ce contrôle, connu en soi, consiste à faire entrer par l'utilisateur son code confidentiel (CC) au clavier (CE2) du milieu extérieur (2), à transmettre ce code confidentiel à la carte (1) qui va le comparer avec le code confidentiel enregistré dans sa zone de mémoire (M11). S'il n'y a pas égalité ou une relation prédéterminée entre ces deux codes, le dialogue est automatiquement interrompu entre la carte et le milieu extérieur.

Conformément à l'invention, ce premier contrôle s'il existe est supposé satisfait.

Un deuxième contrôle peut consister à faire habiliter la carte par le milieu suivant le principe d'un système d'habilitation antérieur tel que décrit précédemment. Plus précisément, le milieu extérieur (2) envoie un nombre aléatoire (E) à la carte (1). Ce nombre aléatoire est généré par un générateur (non représenté) du milieu extérieur. Les circuits de traitement (T1) de la carte (1) calculent un résulat (R1) fonction d'au moins deux paramètres et tel que :

$$R1 = f(E, S1)$$

où (S1) est la clé secrète enregistrée dans la zone de mémoire (M11) et (f) est un algorithme de calcul traduit sous la forme d'un programme (P) enregistré dans cette même zone de mémoire (M11).

Le milieu extérieur (2) prélève le résultat (R1) et le compare avec un résultat (R2) calculé par le milieu extérieur (2) et tel que :

$$R2 = f(E, S2)$$

où (S2) est la clé secrète enregistrée dans la zone de mémoire (M21) et (f) est le même algorithme que

précédemment correspondant au même programme (P) enregistré dans la zone de mémoire (M21).

Si les deux résultats (R1, R2) sont identiques ou satisfont une condition prédéterminée, le milieu extérieur (2) aura l'assurance que la carte (1) est bien habilitée pour obtenir la délivrance du service ou l'accès demandé. Cette condition ne peut être satisfaite que si les clés secrètes (S1, S2) sont identiques ou satisfont entre elles une relation prédéterminée.

Dans le cadre de l'invention, ce contrôle s'il existe est supposé satisfait.

Le contrôle visé par l'invention consiste à faire habiliter le milieu extérieur (2) par la carte (1). Le principe de ce contrôle va être décrit ci-après en reprenant en partie le principe du deuxième contrôle décrit précédemment.

Le nombre aléatoire (E) est fourni et géré par la carte (1) et transmis au milieu extérieur (2). Le nombre aléatoire peut être constitué par une information variable (Eu) prélevée dans la zone de contrôle (M12) de la carte (1) suivant le principe suivant qui est donné à titre d'exemple.

La zone de contrôle (M12) comprend n mots et le contenu de cette zone est modifié après chaque utilisation de la carte, c'est à dire à chaque fois que cette dernière est connectée à un appareil ou à un système. La modification peut consister à changer l'état d'au moins un bit de cette zone après chaque utilisation, et l'information variable (Eu) prise comme nombre aléatoire est le mot de la zone mémoire qui contient le dernier bit modifié lors de la précédente utilisation de la carte.

L'information (Eu) gérée par la carte (1) est transmise au milieu extérieur (2). Les circuits de traitement (T2) du milieu extérieur exécutent le programme (P) précité pour calculer un résultat (R2) au moins fonction des deux paramètres (Eu, S2) et tel que :

$$R2 = f(Eu, S2)$$

De son côté, les circuits de traitement (T1) de la carte (1) exécutent le même programme (P) pour calculer un résultat (R1) au moins fonction des deux paramètres (Eu, S1) et tel que :

$$R1 = f(Eu, S1)$$

Ensuite le résultat (R2) est transmis à la carte (1) pour être comparé au résultat (R1).

L'habilitation du milieu extérieur (2) par la carte (1) ne peut être validée que si les clés secrètes (S1) et (S2) sont identiques ou satisfont une relation prédéterminée.

La cohérence des résultats (R1, R2) peut être simplement une relation d'égalité entre eux vérifiée par un circuit comparateur (3) de la carte (1) relié au bus (b1), ce qui suppose que les clés (S1, S2) sont identiques. En variante, la cohérence des résultats (R1, R2) peut être satisfaite au travers d'une relation prédéterminée entre (R1) et (R2) ou d'une même relation satisfaite par (R1) et (R2). Cette relation est traduite par un programme (PO) enregistré dans la zone (M11) de la mémoire (M1) et qui est exécuté par les circuits de traitement (T1) de la carte (1).

S'il n'y a pas identité des résultats (R1, R2) ou cohérence entre ces deux résultats, le dialogue est interrompu entre la carte (1) et le milieu extérieur (2). Cette interruption est sous le contôle de la carte (1).

On va maintenant décrire trois types de programmes (P) qui peuvent être utilisés pour calculer les résultats (R1, R2).

Un premier type de programme (P) peut être la mise en oeuvre d'un algorithme non inversible. Dans ce cas et par mesure de sécurité, il est souhaitable que le milieu extérieur soit physiquement protégé dans un module de sécurité pour éviter à un fraudeur de prendre connaissance du programme (P) et de la clé secrète (S2).

Un second type de programme (P) peut être la mise en oeuvre d'un algorithme inversible du type connu sous le nom de "DES". Le programme (P) se décompose alors en deux programmes (P1, P2) qui correspondent respectivement aux fonctions directe et inverse de l'algorithme.

Plus précisément, la carte (1) communique l'information (Eu) au milieu extérieur qui va exécuter par exemple la fonction inverse (programme P2 enregistré dans la zone de mémoire M22) pour calculer un résultat chiffré (R2) tel que :

$$R2 = f2^{-1}(Eu, S2)$$

où (S2) est la clé de chiffrement de l'algorithme. Ce résultat (R2) est transmis à la carte (1) qui va exécuter la fonction directe de déchiffrement (programme P1 enregistré dans la zone de mémoire M11) sur ce résultat (R2) pour calculer une information (Eu1) telle que :

$$Eu1 = f2\ (R2, S1)$$

où (S1) est la clé de déchiffrement de l'algorithme préenregistré dans la zone de mémoire (M11). Ensuite la carte (1) vérifie que l'information (Eu1) correspond bien

à l'information (Eu) qu'elle a précédemment transmise au milieu extérieur.

En variante du second programme (P), les circuits de traitement (T2) du milieu extérieur (2) exécutent la fonction inverse (programme P2) pour calculer un résultat chiffré (R2) tel que :

$$R2 = f2^{-1}(R, Eu, S2)$$

où (R) est un résultat prédéterminé enregistré dans les mémoires (M11, M21) de la carte (1) et du milieu extérieur (2).

De leur côté, les circuits de traitement (T1) de la carte (1) exécutent la fonction directe de déchiffrement (programme P1) sur ce résultat (R2) pour calculer un résultat (R1) tel que :

$$R1 = f2(R2, Eu, S1)$$

Ce résultat (R1) doit concorder avec le résultat (R) prédéterminé ou satisfaire une même relation prédéterminée.

Comme pour le premier type de programme, il faut prévoir un module de sécurité pour protéger le programme (P2) et la clé de chiffrement (S2).

Enfin, un troisième type de programme (P) peut être la mise en oeuvre d'un algorithme inversible à clé publique connu sous l'abréviation "R S A". Cet algorithme fait intervenir une clé publique et une clé secrète. En faisant exécuter par le milieu extérieur (2) une fonction de chiffrement avec la clé publique, il n'est plus nécessaire de prévoir un module de sécurité et le milieu extérieur

(2) devient totalement banalisé. Avec ce troisième type de programme, on peut également envisager la variante indiquée avec l'utilisation du deuxième type de programme.

La description fait ressortir que l'information variable (Eu) est prélevée de la zone de mémoire (Z1) de la carte (1) et que cette information est modifiée à chaque utilisation de la carte (1).

D'une façon générale, l'information (Eu) peut être quelconque dès l'instant qu'elle est interne à la carte (1) et qu'elle évolue après chaque utilisation de la carte (1) pour ne jamais être identique à une information (Eu) déjà utilisée.

En variante, l'information (Eu) peut être définie à partir d'un dispositif (4) interne à la carte (1) relié au bus (b1), indépendant de la mémoire (M1) de la carte (1) et qui est capable de produire une information différente à chaque utilisation de la carte (1).

Ce dispositif (4) peut être à titre d'exemple :

- un circuit de comptage qui comptabilise le nombre de fois où la carte a été utilisée,

- un générateur de nombres aléatoires,

- un compteur de temps alimenté par une pile (5), ...

Revendications

1. Procédé d'habilitation d'un milieu extérieur par un objet portatif relié audit milieu, du type consistant à faire respectivement calculer des premier (R1) et second (R2) résultats par des circuits de traitement (T1, T2) de l'objet portatif (1) et du milieu extérieur (2), ces calculs prenant au moins en compte une même donnée variable (Eu), caractérisé en ce qu'il consiste à prélever ladite donnée variable (Eu) dans l'objet portatif (1) et à faire vérifier la cohérence des deux résultats (R1, R2) par l'objet portatif (1).

2. Procédé selon la revendication 1, caractérisé en ce qu'il consiste à prélever la donnée variable (Eu) dans une zone de mémoire (M12) de l'objet portatif (1), cette zone (M12) contenant au moins un champ de n bits dont au moins un bit est modifié à chaque utilisation de l'objet portatif (1).

3. Procédé selon la revendication 2, caractérisé en ce qu'il consiste à prendre pour la donnée variable (Eu) une information de m bits dans la zone (M12), ces m bits contenant le bit modifié lors de la précédente utilisation de l'objet portatif (1).

4. Procédé selon la revendication 1, caractérisé en ce qu'il consiste à prélever la donnée variable (Eu) à partir d'un dispositif (4) indépendant de la mémoire (M1) de l'objet portatif (1), situé dans l'objet portatif (1) et dont l'information de sortie est différente à chaque utilisation de l'objet portatif (1).

5. Procédé selon la revendication 4, caractérisé en ce qu'il consiste à prélever la donnée variable (Eu) à partir d'un circuit de comptage (4) dont le contenu est modifié à chaque utilisation de l'objet portatif (1).

6. Procédé selon la revendication 4, caractérisé en ce qu'il consiste à prélever la donnée variable (Eu) à partir d'un générateur de nombres aléatoires (4) situé dans l'objet portatif (1).

7. Procédé selon la revendication 4, caractérisé en ce qu'il consiste à prélever la donnée variable (Eu) à partir d'un compteur de temps (4) situé dans l'objet portatif (1) et alimenté par une pile (5).

8. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il consiste pour vérifier la cohérence des deux résultats (R1, R2), à les comparer dans un circuit comparateur (3) situé dans l'objet portatif (1).

9. Procédé selon l'une des revendications 1 à 7, caractérisé en ce qu'il consiste pour vérifier la cohérence des deux résultats (R1, R2), à définir une relation de cohérence déterminée, à traduire cette relation par un programme (P0) enregistré dans la mémoire (M1) de l'objet portatif, et à faire exécuter ce programme (P0) par les circuits de traitement (T1) de l'objet portatif (1).

10. Procédé selon l'une des revendications 1 à 7, caractérisé en ce qu'il consiste à faire respectivement calculer les résultats (R1, R2) par les fonctions de chiffrement et de déchiffrement d'un algorithme inversible tel qu'un algorithme à clé publique.

11. Procédé selon la revendication 10, caractérisé en ce qu'il consiste à faire calculer le résultat (R2) par application de la fonction de chiffrement (f2) de l'algorithme précité qui prend au moins en compte la donnée variable (Eu) et un résultat prédéterminé (R), à faire calculer le résultat (R1) par application de la fonction inverse de déchiffrement ($f2^{-1}$) dudit algorithme

sur le résultat (R1) et la donnée (Eu), et à faire vérifier par l'objet portatif (1) la cohérence du résultat (R1) par rapport au résultat (R).

12. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il consiste à faire prendre en compte dans le calcul des résultats (R1, R2), une donnée (S1) propre à l'objet portatif (1) pour le calcul du résultat (R1) et une donnée (S2) propre au milieu extérieur (2), ces données (S1, S2) devant être identiques ou devant satisfaire une relation déterminée entre elles.

1.1